Location-sharing Model in Mobile Social Networks with Privacy Guarantee

Tiago Antonio Rosa and Sergio Donizetti Zorzo
Computer Science Department, Federal University of São Carlos, São Carlos, SP, Brazil

Keywords: Privacy, Mobile Social Networks, Rules of Privacy, Location-sharing.

Abstract: Mobile social networks allow users to access, publish, and share information with friends, family, or groups of friends by using mobile devices. Location is one kind of information frequently shared. By using location-sharing on a social network, users allow service providers to register this information and use it to offer products and services based on the geographic area. Many users consider offers a personal gain, but for others, it causes concerns with security and privacy. These concerns can eliminate the use of mobile social networks. This paper presents a model of a mobile social network with a privacy guarantee. The model enables the user to set rules determining when, where, and with whom (friends or a group of friends) location information will be shared. Moreover, the model provides levels of privacy with anonymity techniques which hide the user's high-accuracy current location before it is shared. To validate the model, a mobile social network prototype, MSNPrivacy (Mobile Social Network with Privacy), was developed for Android. Tests were carried out aiming to measure MSNPrivacy's performance. The results verify that the rules and privacy levels in place provide an acceptable delay, and the model can be applied in real applications.

1 INTRODUCTION

Mobile social networks have grown immensely due to hardware improvements and the reduction of costs to buy mobile devices. This is verified through Facebook, which boasts 1.4 billion users worldwide who are frequently checking the latest updates and sharing interests with friends and family (Statistic Brain, 2014). Mobile devices represent a simple way to share information, such as location, with other people.

By using location-sharing on a mobile social network, the user not only provides his current position to friends and family, but also allows the net to register this location information. This information enables the social network to offer and advertise products and services near his geographical area.

Location-sharing enables the social network to offer recommendations, which some users consider beneficial, while others find it a privacy concern. Furthermore, malicious users can easily join the social network and, in this way, get locations of other users. In possession of this information, these malicious users can pose a serious threat to the privacy of other users. Evidence of such concerns can be seen in related works (Toch et al., 2010); (Benisch et al., 2010), and they can affect the users initiative in using these applications. Some mobile social networks, like Facebook, already offer privacy control to their users when using a certain application. This control is carried out with respect to established privacy policies that determine which social network users can know a person's location and in which places, dates, and times this information can be published. Such policies established by social networks, when existing, are implemented with limitations in relation to offering the real user location and the group of users.

This paper presents a location-sharing model for mobile social networks with a location privacy guarantee for individual users and groups of users. Users can customize privacy through levels and rules. The levels define the accuracy of the location which will be shared, and the rules define where, when, and with whom the user location will be shared. The motivation for the development of this model was to minimize the risks to users' privacy in the use of Social Networks Furniture. Such risks allow users' identities to be gauged through the

Antonio T. and Donizetti Zorzo S..
Location-sharing Model in Mobile Social Networks with Privacy Guarantee.
DOI: 10.5220/0005383200440054
In *Proceedings of the 17th International Conference on Enterprise Information Systems* (ICEIS-2015), pages 44-54
ISBN: 978-989-758-098-7
Copyright © 2015 SCITEPRESS (Science and Technology Publications, Lda.)

location; moreover, their safety may be compromised, as the location history allows to obtain the path performed.

The proposed model was validated through implementation of a prototype for a mobile social network called MSNPrivacy (Mobile Social Network with Privacy). MSNPrivacy allows the user to share his location with members of his social network or with groups created by the user himself or those created automatically, taking into account certain contexts such as the degree of relationship or the geographic position.

Tests were carried out with the aim of measuring the model's performance. Results show the delay provided by privacy techniques is acceptable, and the model not only has a satisfactory answer time, but can be implemented in real applications.

The paper is organized as follows: Section 2 presents a discussion about related works; Section 3 presents a privacy context for location-sharing in mobile social networks; Section 4 presents the proposed model and its architecture; Section 5 presents the mobile social network prototype implemented from the presented model, MSNPrivacy; Section 6 presents the results obtained in performance tests; Section 7 presents the results obtained in usability estudy and; Section 8 presents the conclusion and future works.

2 RELATED WORKS

A great effort has been made by several authors on the subject of information-sharing privacy in mobile social networks. Some of these works were imperative to developing the model proposed in this paper.

Smith et al., (2005) carried out an initial investigation on technologies which allow people to share their location in mobile social networks. The result of this work was the development of a system called Reno. This system allows its users to manually share their location with other people and to pre-define locations or regions. Reno uses SMS to notify the location inside the social network, and the coordinates are obtained through the triangulation of cell phone towers. These technologies were used due to the high cost of the most modern devices with GPS. The privacy controls in the Reno system are performed only when the user decides to share his location. The proposed model in this paper, besides considering when the user wants to share his location, privacy levels are offered, with each having a defined characteristic to guarantee the high-accuracy location remains hidden.

Toch et al., (2010) presented Locaccino, a location-sharing application for mobile social networks which allows the user to define rules to publish his location information. These rules are defined considering the person, the time, and if the user is willing to share his current position. However, the shared location is high-accuracy information. The proposed model, besides considering the aspects approached in the Locaccino application and also allowing for the definition of rules, applies algorithms which guarantee the current location's anonymity.

Bilogrevic et al., (2013) investigated users' preferences in sharing their location in mobile social networks. The authors made use of users' behaviors when sharing their locations, and the result obtained was that users cannot specify correctly their location-sharing preferences. From that information came the creation of SPISM, a location-sharing system that (semi) automatically selects which rule must be applied when a user receives a request to share his information. Rule selection is made using machine learning algorithms. However, as with the other works, SPISM publishes high-accuracy location information. The proposed model does not use machine learning algorithms to select the best rule for the location-sharing requirement. Instead, it enables the user to manually set the rules to be applied with each user or one of his groups. Moreover, the model allows the user to match his sharing preferences with levels which apply algorithms to hide the high-accuracy location before it is shared.

Ribeiro and Zorzo (2009) presented the LPBS (Location Privacy-based System), a system based on levels which guarantee users' location privacy in LBS. This system is divided into levels, with each level having distinct privacy characteristics that guarantee high-accuracy location anonymity. However, while the LPBS guarantees users' privacy in LBS, it is not applied in mobile social networks. The proposed model uses levels which guarantee a user's location anonymity and matches these levels with publishing preferences.

3 PRIVACY

Privacy concerns were not caused by the emergence of computers and the internet, rather, they existed long before. Computers, the internet, and the wide storage of data it enabled made it possible to collect, process, and transmit large volumes of data,

including personal data. Current privacy studies generally involve different dimensions: law, ethics, and information technology (Benisch et al., 2011).

The most accepted definition of privacy is the right of users, groups, or institutions to determine when, how, and to what extent their information is communicated to others (Bilogrevic et al., 2013). This definition captures the idea that privacy is not simply the lack of information about the user, rather, it is the control users must have of information related to them.

Location privacy is defined by Xu et al., (2010) as a special kind of information privacy concerning an individual's claim for determining when, how, and to what extent location information about them is communicated to others (Toch et al., 2010). The person whose location is being measured must have control of when it is published and who can view it. Access to user location information must be available only as per a user's privacy preferences (Toch et al., 2010).

In this paper, privacy is understood as the user's right to use mobile social networks and define where, when, and with whom his location will be shared, as well as the accuracy of this information.

When using mobile social networks, the user may share his interests and location with friends, family, and co-workers. However, with the increasing use of these applications, users' concerns related to privacy issues have also increased.

All of the content posted, especially the location, can be accessed or shared by other entities, which represents the origins of privacy attacks. Gao et al., (2011) considered these origins as gaps; they can be classified as follows: (i) other users of the social network, (ii) third-party applications, and (iii) the actual service provider.

Other users of the social network pose a threat due to the ease that attackers have in joining the social network, creating an account on the service provider and becoming an authentic user. These malicious users can also produce false context information for the RSM to gain access to resources, gain a temporary identity, and to integrate user groups that are automatically formed by the Mobile Social Network.

Third-party applications are developed using the Application Programming Interface (API) available from the Mobile Social Network. The API provides an open interface for the creation of new resources in the Mobile Social Network. These applications are developed by third parties and therefore are not always reliable. Third-party applications can be games, music applications, photos, videos, and applications used by advertising agencies to carry out campaigns promoting products and services. These applications grant the user free access permission to personal information such as shared locations, move history, etc.

The social network service provider is responsible for providing the necessary resources to users of the Mobile Social Network. This person has access to all of the personal information relating to users who have been issued or published. For this reason, users are left to rely on the service provider and are becoming more and more concerned about not really knowing who is manipulating their information.

Previous works (Benisch et al., 2011); (Smith et al., 2005); (Bilogrevic et al., 2013) show that users feel more comfortable when they know who they are sharing information with. These preferences can be easily reached through a white list or creation of a list of people the users would be willing to share their information with. However, a user's preferences are beyond the simple use of these lists (Benisch et al., 2011).

In 2009, Toch et al., (2010) noted that users have common preferences such as, "I am willing to share my location with my friends during the week, nine to five, and only when I am at my workplace". This consideration can be established by rules in the application that is being used or the human computer interaction or in an intermediate mechanism device.

Research has been carried out to try to discover patterns of behaviors and location-sharing preferences (Benisch et al., 2010); (Toch et al., 2010). These research results show that privacy goes from simple to the most complex. The resulting preferences are listed below (Benisch et al., 2010):

- White Lists: Allow users to indicate specific members of their social network with which they feel comfortable sharing their location. This is the simplest privacy definition considered.
- Places: Allow users to indicate specific places where they feel comfortable sharing their location with members of their social network. This preference is considered more complex than white lists.
- Times: Allow users to indicate the time period they feel comfortable sharing their location with members of their social network. As with place preference, time preference is more complex than the white list.
- Days: Allows users to indicate which days of the week they feel comfortable sharing their location with members of their social network.

Users can match the preferences presented above, increasing the complexity further.

The model proposed in this paper encompasses the preferences described above and enables users to create privacy rules using one or more preferences. Moreover, the model provides levels which provide accuracy and anonymity of the location to be shared. Matching the preferences and the privacy levels, a user can reduce his risks when sharing location information.

4 MODEL

Figure 1 illustrates the mobile social network model proposed in this work which provides a privacy guarantee. It is composed of a client application working in mobile devices, a social network server (SNS), a reliable proxy, and users.

The application working in mobile devices must be able to connect to the internet through Wi-Fi networks or a data plan from operators, connect to servers, and determine its location through GPS, triangulation, and a Wi-Fi signal. Moreover, the devices must be able to receive location requirements and process rules and techniques which guarantee users' privacy.

Figure 1: Model architecture.

The social network server, illustrated in figure 1 by Mac B, meets user requests. The main goal of the server is to allow users to find the current IP address of social network members whenever they require send a request of location. For that, the server stores a list of its users, their contact lists, and the updated IP addresses of each user. Moreover, the server stores the current status of users. Users interact with the server when registering (only once), during the login phase (every time a user connects or disconnects), when downloading a list of contacts, when periodically informing the updated IP address and its status, and when sending location requirements to a member of their net.

In the model, users can be classified in two different ways: a requester, when sending a request to another user, or a target, when receiving a location-sharing request.

To increase communication safety, all requests made between users and the social network server are encrypted with a public key certificate obtained from a reliable Certification Authority (CA).

To protect users' location privacy in relation to the server, none of the privacy techniques are applied by the server, but instead by the application in the users' devices. The information is sent to the server only after necessary alterations; this way, the server cannot know the real user location. This is a crucial aspect of the model, as it does not permit the server, which can be outsourced, to have any information relating to a user's location. However, the server knows their IP address and can, therefore, accurately infer their location (based on the IP-geolocalization). To solve this problem, users can hide their IP address using a reliable proxy which is illustrated in figure 1 by Mac A.

In this model, the privacy rules defined by the user consider the position, period (in hours), days of the week and whitelists. Other rules may also be incorporated in the model.

The main goal of the model is to guarantee the privacy of users who share their location with members individually or with an existing group in their social network. For that, besides meeting the users' preferences presented above, the model implements mechanisms which guarantee privacy through anonymity and the hiding of high accuracy positions. The model offers privacy on three different levels, allowing the user to personalize privacy settings according to his needs and interests. The details of each level are described as follows.

4.1 Level 1 – Accuracy Adjustment

The accuracy adjustment technique (Ribeiro and Zorzo, 2009) consists of modifying the high accuracy location so that this information about position represents different points inside a certain area. This adjustment is calculated based on the original location's random displacement for any direction inside a given radius, as shown in figure 2.

In Figure 2, the real user location is illustrated by the center circle A; the displacement radius is illustrated by the letter 'r'. When the accuracy is

adjusted, the user's location is randomly displaced for any direction inside the area illustrated by the smaller circle B. The displacement radius or accuracy adjustment coefficient is defined by the user according to his preference.

To perform the accuracy adjustment, the formula below was used. It is based on the spherical triangle formed by the initial point, the final point, and the north pole (Hochbaum and Shmoys, 1985); (Smart, 1977).

Two sides of this triangle are already known: the side between the initial point and the north pole and the side referring to the displacement distance. In addition, the angle formed by these two sides is also known, and it is characterized by the displacement direction.

$$lat2 = \arcsin(\sin(lat) * \cos\left(\frac{d}{R}\right) + \cos(lat1) * \sin\left(\frac{d}{R}\right) * \cos(\theta)$$

$$dlon = arctan2(\sin(\theta) * \sin\left(\frac{d}{R}\right) * \cos(lat1), \cos\left(\frac{d}{R}\right) - \sin(lat1) * \sin(lat2))$$

$$lon2 = mod(lon1 - dlon + pi, 2 * pi) - pi$$

In the formula above, the θ element represents the displacement direction where lat1 and lon1 are the coordinates of the initial point, and the angular distance is illustrated by d/R, where d is the adjustment distance set by the user and R is the Earth's radius. The goal of the module applied in the end of the formula is to accommodate cases in which the points are in opposite meridians. The resulting coordinates are illustrated by lat2 and lon2. This formula is valid only for cases in which the calculated distance is less than a quarter of the Earth's circumference.

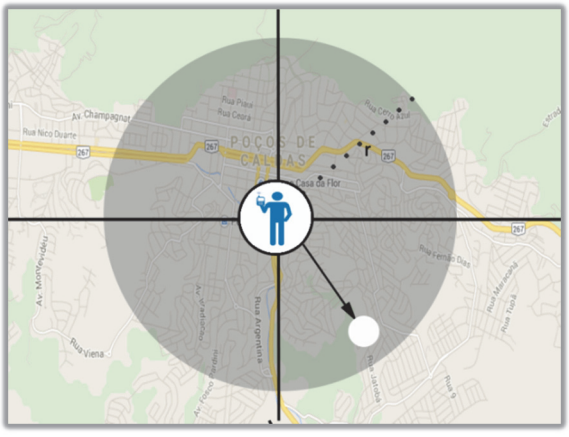

Figure 2: Accuracy adjustment.

After performing the accuracy adjustment in the user location information, the application sends the resulting coordinate to the SRS.

This technique guarantees that user location information shared with friends or a group of users inside a social network will not be a high accuracy location, and in this way, level 1 guarantees a certain amount of privacy to users.

Users can still match the accuracy adjustment in level 1 with the privacy preferences presented in Session 2 specifically to place, day of the week, and break time.

4.2 Level 2 – Anonymity

The model in level 2 guarantees user anonymity through a location information hiding technique. To hide information, information about the location of online users who are geographically near is used. In the case of a group defined inside a social network, the coordinates of the users in the group are used. To obtain the necessary locations so the anonymity technique can be applied, the application requests the locations of other users.

The hiding location is calculated by selecting one of the online groups' locations. This selection is made by calculating the fair point, a location which reduces the distance of any user related to all others. For calculating the fair point, the k-center problem was used. In the k-center problem, the goal is to find the k site among all locations shared so that the maximum distance of any user in relation to the others is reduced. Figure 3 illustrates an example of a scenario modeled with the k-center problem, where the fair point is calculated with four users.

In figure 3, the traced lines represent the maximum distances, while the full line represents the minimum distance among all the maximum distances. Therefore, in this scenario, the fair point is User 2.

After selecting the location which will hide the user's real position, the accuracy adjustment technique in level 1 is applied in the selected location and shared after being changed. The accuracy adjustment is necessary because the location which will be shared is a high accuracy location and is a valid location of a social network user.

The anonymity technique of this level cannot always be applied because it depends on the locations of other users within the group. If these locations are not obtained within five seconds, the application fine-tunes the current position of the user and conceals the actual location of the user.

Figure 3: Scenario modeled with the k-center problem.

4.3 Level 3 – Anonymity Guaranteed

In level 3, the model guarantees the existence of the anonymity group through the false location technique (Ribeiro and Zorzo, 2009), as illustrated in Figure 4.

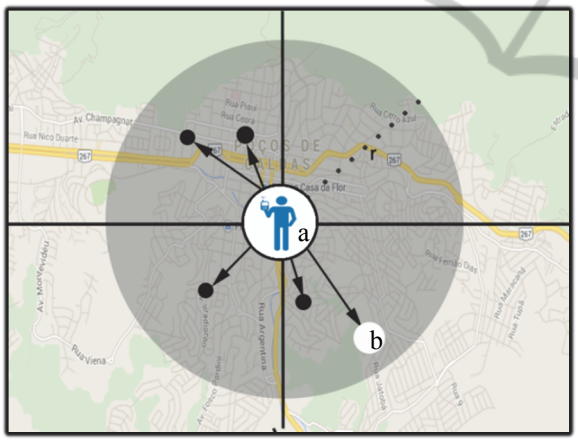

Figure 4: Generation of false locations.

The client application gets the current position of the user, shown in Figure 4, at circle "a" using the device's GPS. From this information, the application generates four other false locations, shown in Figure 4 by dark circles, using the characteristics of the level of precision adjustment technique 1. After this process, the application has five locations (four false and the current user). Then, the same technique is applied to compute the level 2. Anonymity is also applied at this level. The resulting location of anonymity, represented by circle "b" in Figure 4, is fine-tuned and then shared in the social network. The model guarantees the user's privacy because the shared location will not be his real coordinate.

All techniques applied are performed on the user's device itself to guarantee the server cannot obtain the user's real location; the shared location is not real.

Users can even combine privacy levels with their sharing preferences.

The proposed model was validated by the implementation of a prototype for a mobile social network called MSNPrivacy (Mobile Social Network with Privacy). MSNPrivacy allows the user to share his location with individual members of his social network or with groups created by him or automatically, taking into account a given context, for example, the relationship or geographic position. Details about MSNPrivacy's operation will be discussed in the next session.

5 MSNPrivacy

MSNPrivacy(Mobile Social Network with Privacy) is a mobile social network application prototype implemented in Android (2014) which was developed with the aim of validating the proposed model. In the prototype implementation, the simple and intuitive natures of social networks were considered as far as usability. To compose the user's mobile social network, the prototype uses Facebook's friends lists. Figure 5 shows the main application interfaces where users can login and register, see the list of contacts and the status, require the location and see the feedback, and set their preferences and privacy levels.

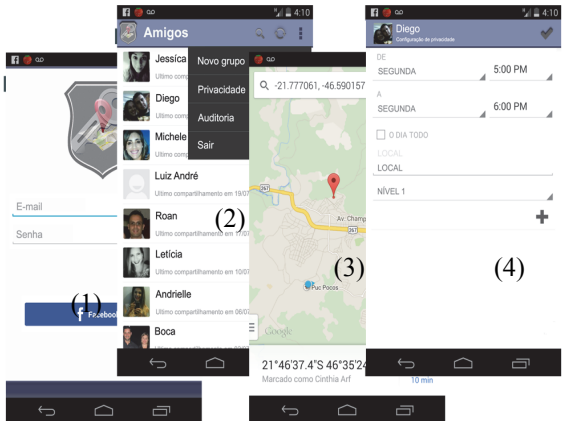

Figure 5: Main MSNPrivacy application interfaces.

5.1 Operation Principle

MSNPrivacy works as follows: First, the user logs in or registers on the server, providing the access login and password. The application also provides the

option to register directly through Facebook as shown in figure 5 (1). If the user is connected to Facebook, the application directly captures the login information with no need for it to be typed by the user. At this point, in addition to sending the data to the server, the application starts a service which periodically updates the current IP address and also starts another service which monitors the reception of location requests from other users of the social network. After obtaining the user login data, the application sends it to the server. The server receives the data and, if the user is not registered, the server promotes integration with Facebook, looking for the user's list of contacts. After obtaining the contacts, the server stores them and sends them to the user's device which locally stores the contact list and presents it to the user. The process referring to the user's first access is presented in the sequence diagram in Figure 6.

The user can set his preferences and privacy levels for each contact of his list and for the groups he is in (figure 5 (4)). If this setting is not performed, the application uses level 1 as the pattern for all contacts and groups.

In a typical scenario, the User requests one of his online contacts' location by selecting him from his list. Next, the application prepares the request and sends it to the server. The server looks for the requested user's current IP, connects to the device, and sends the request. After receiving the request, the application verifies the privacy preferences set for the requested user, applies the privacy techniques on the obtained location, encapsulates the data, and sends it back to the server. The server directs the result to the Uses and shows the location on a map after receiving the information. If the requested user is not online at that moment, the requested user's application comes back to the main interface, and when the server receives the requested user's data, it sends it to the User's device. As soon as the application receives the feedback, it notifies the User. The requirement information received or sent is stored either in the server or in the user's device. This way, users can audit in the application or on the web. The process related to the location requirement is presented in the sequence diagram in figure 7.

All privacy techniques presented in each level are processed in the user's device. This ensures the server does not have access to high-accuracy location information which is shared on the social net. However, the server still has the user's IP address which makes it is possible to infer his location. This issue can be easily solved using a reliable proxy as long as one is available.

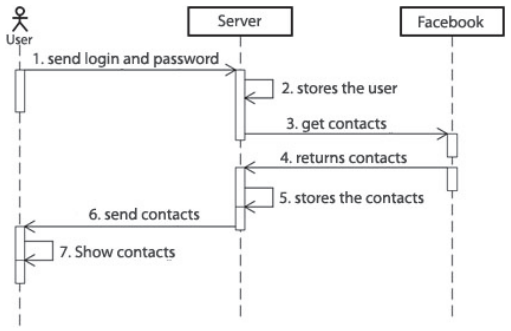

Figure 6: First access sequence diagram.

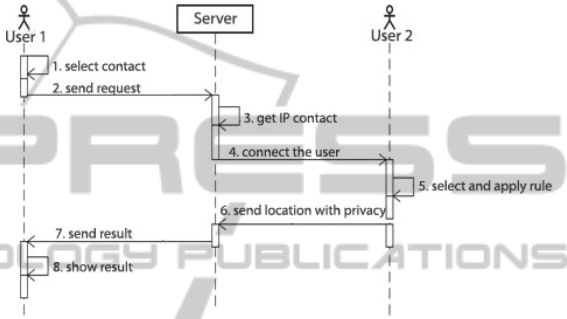

Figure 7: Location request of a contact.

5.2 Privacy Preferences Setting

The application allows the user to set his privacy preferences with each member of his social network and within the groups he has joined (figure 5 (4)). Moreover, the user can match his preferences with the privacy levels offered.

The proposed model allows to define rules. In MSNPrivacy some rules such as "Who", which allows the user to indicate which member of its mobile social network feels the urge to share his position, "Time", which allows to determine the period of schedule was implemented, "Where", which to determine the location and "days" which enables want to determine the day or days of the week that your location will be disclosed.

To better illustrate the privacy setting, a hypothetical user called "Alice" will be considered. Alice wants to share her location with friends in her social network when she is at home and on the weekends from 9:00 a.m. to 5:00 p.m. In this case, when creating a setting, Alice will have to indicate the location, the period of time, and the days of the week. Alice can even specify the privacy level. In case no level is specified, level 1 is automatically used. Alice will be able to create a rule for each member or group (individually) in her social network or set a rule for everybody.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

The model deals with the conflict rules in two ways. In the first case, the model allows the user to only create rules that grant sharing your location and does not allow the creation of rules that deny sharing. For example, "Mary can see my location from 9 AM to 5 PM," but she is not allowed to specify, for example, that "my friends cannot see my location on the weekends." In the second case, the rule is checked before it is committed. This check is performed to prevent the rules from having conflicting parameters. For example, "Mary creates a rule that allows your friends to see your location on the weekend," so she failed to create a new rule that specifies that "your friends can see your location on weekends from 9 AM to 5 PM."

6 RESULTS

Aiming to measure the model's performance, tests on the main options available in each level were carried out, such as the first access, where the integration with Facebook took place, location request, and the privacy techniques.

To perform these tests, the Android operational system emulator with IDE Eclipse and the ADT plugin were used to perform the application prototype. For the provider, a machine with a Windows 7 operational system (2GHz CPU, 3GB RAM) was used.

Figure 8 presents the model's performance when the user registers. The result indicates that running time increases in correspondence with the number of contacts the user has on Facebook. This happens because the moment the user registers, the application makes an authentication with the server. The server then promotes integration with Facebook with the goal of looking for and registering all the user's contacts that are popular in his mobile social network. Runtime time can also vary according to the internet connection used. As this action is carried out only when the user registers, it does not disturb the model's performance.

The following results show the model's performance for each privacy level.

Figure 9 presents the model's performance when applying the accuracy adjustment in level 1. As can be seen, the average runtime is constant, taking 0.3 seconds. This is because the accuracy adjustment calculation is always applied on the user's individual location and not in a group of users. Therefore, the number of users does not have an influence on the outcome. What can impact running time is communication with a GPS and the internet connection quality.

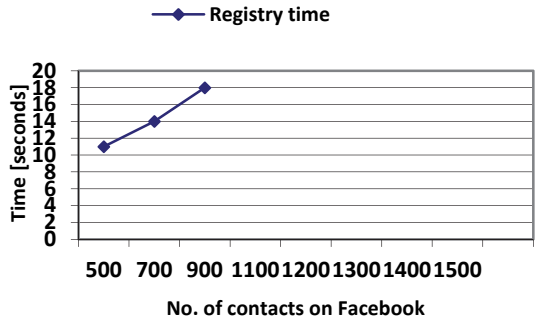

Figure 8: Runtime time during user registration.

Figure 10 shows the model's performance when applying privacy techniques in levels 2 and 3. As can be seen, as the number of users in a group increases, the runtime also increases. This happens because to have anonymity, the algorithm in these levels uses location information from all users in the group.

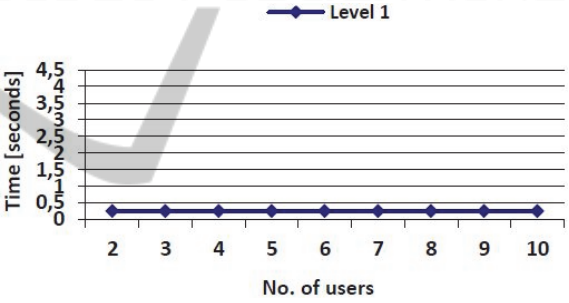

Figure 9: Level 1 Runtime.

The difference in the runtime in level 3 occurs because, in this level, besides calculating the anonymity, the MSNPrivacy generates false locations using the accuracy adjustment and applies this same technique in the user's high-accuracy location.

As in the other results, the runtime in levels 2 and 3 can change depending on the internet connection quality or the GPS sign quality. Moreover, depending on the privacy rule set by the user, the running time can increase. However, this time does not put the model performance at risk.

Figure 11 illustrates the runtime results of the tests with rules. Tests to measure the performance of the model were realized based on the number and type of rule. These tests considered the worst-case scenario: one rule configured with all of the possible parameters and all of the rules with all of the possible parameters. In this test, we took three measurements based on the number of rules (10, 100, and 1,000 rules) configured with all of the

possible parameters. The average time spent with 10 rules was 14 seconds; with 100 rules, the average time was 25 seconds; with 1,000 rules, the average time spent was 60 seconds. These results were plotted on a graph in Figure 11 (new version). In this figure, we draw the trend line to get the behavior of the system performance based on the number of the rules. Analyzing these results, we conclude that for a set of rules (n) to infinity, time behavior tends to increase linearly (i.e., the model runtime with no set rules is O (n)).

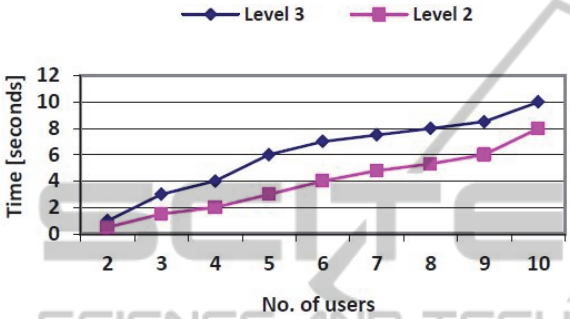

Figure 10: Runtime in levels 2 and 3.

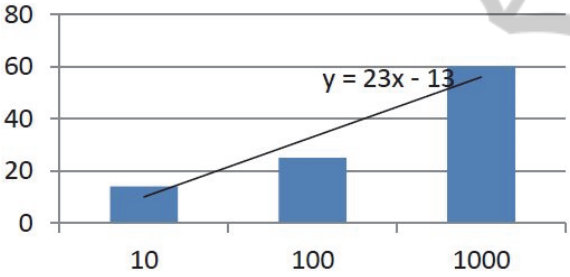

Figure 11: Runtime time x number of rules.

Based on the results obtained from the tests carried out in the privacy levels and testing with the rules, the average delay added by the implemented prototype was 35 seconds. This delay time is proportional to the implementation of level 2 and 3, with 10 users per group. The inserted delay can vary according to the number of users in a group. In a group with more than 100 users, the implementation of level 2 can become unwieldy. The solution to this problem is to adjust the amount of locations used in the calculation of anonymity. Level 3 is not compromised in this case because the locations used are generated by the application; the initial number of points generated is four.

Although a delay is inserted in the model performance, it is safe to say this delay does not damage the usability of the mobile social network, since the delay will only happen when the user receives a request for publishing his location. With the other functionalities, there will be no delays in performance. Furthermore, test results show that the delays generated by the privacy techniques offered are at proportional and justifiable levels; further, the privacy rules are desirable and chosen by users.

7 USER STUDY

A usability study was conducted to get the users' perceptions of and measure the effectiveness of the privacy mechanisms the model offered. The study was conducted with 50 participants, aged 19 to 30 in the exact sciences, health, and humanities. A previous study found that many of the problems that are likely to occur in a given population were only identified by five participants (Leon, 2012). We asked the participants to answer questionnaires. The issues addressed in the questionnaires were designed to measure user satisfaction related to privacy and usability.

The study consisted of two phases. In the first phase, participants answered an initial questionnaire composed of nine questions. The objective of the first questionnaire was to measure the level of participants' understanding of privacy in mobile social networking. In addition, the responses from this survey will be compared with the responses to the second questionnaire. In the second phase, participants used the main features of the prototype to create rules and privacy levels, location, and to request access to audit. Then, we asked participants to answer the second questionnaire, which contained 21 questions. The objective of this phase was to obtain feedback from participants on the usability and efficiency of the privacy techniques offered. A five-point Likert scale (where one means strongly agree and five means strongly disagree) was used.

The results of the study show that, at the beginning of the tests, 77% of users had mistaken understanding of privacy in mobile social networking or did not worry about privacy issues. The results at the end of the tests show that 100% of the participants believed that privacy safeguards were important and influenced location-sharing decisions in mobile social networking. Regarding the privacy techniques the model offered, 87% of participants approved of its efficiency, while the rest of the participants (13%) did not approve or were indifferent. On the usability of the prototype, 76% found it difficult to configure privacy rules and levels the way the prototype offered. Overall, 80% of participants would use the mobile social network prototype in their day-to-day lives.

8 CONCLUSION AND FUTURE WORKS

Mobile devices represent a simple way to quickly share information with other people and the use of mobile social networks is a easy way to share location.

When a user shares his location with friends and family on a social network, he also allows this information to be registered by the social network itself, which then uses it to offer products and services according to location. For many users, this offer is seen as a benefit, but for many, privacy concerns outweigh that benefit. These concerns can reduce motivation to use social networks.

The privacy offered by the model through the definition of rules and levels prevents users from attacks mentioned in section 2. As the shared location information are hidden throughout the levels, malicious users do not get the information real position and with high accuracy user. Thus, hinders your identity is inferred by location. In addition, the social network provider does not store the history of shared locations and thus cannot to trace the stream of the users. The other members of the social network store all locations shared your friends, however, is very difficult to get the user path if it has set policies and levels for the share.

An interesting point to note is that the model does not fully committed services and recommendations offered by the social network, therefore users allow their location to be shared according to the rules. The location modified by levels still belongs to the geographical area where the user is. Thus, services and offers recommendations based on geographic area can still be made. But personalization is the user's responsibility, since it allows its position to be shared, services and recommendations made by the social network will not be compromised.

The results show that the model has good performance, despite the existence delays. Analysing the worst case, the model runtime to process an incoming request is on average 28 seconds. This delay added to the implementation of the social network is acceptable when compared to the average time spent by the GPS to obtain the first location that is 30 seconds. The test results also show that delays generated by using the privacy techniques are proportionate to the desired levels of privacy of user.

The results obtained in the evaluation of users show three important points: First point is that users believe that, for the use of mobile social networks, supply and privacy safeguards is essential. The second point is that most users approved the efficiency of privacy techniques offered by the model. However, despite the privacy of efficiency is approved, the prototype needs improvements over its usability.

Among the future works are: The need to move employees algorithms in the privacy level 2 in order to improve application performance; The way users perform the privacy rules setting should be optimized using the results of the usability study; Evolve the prototype is makes it the closest to an application of real mobile social network and, finally, conduct a study to measure the configuration preferences user privacy.

REFERENCES

http://www.statisticbrain.com/social-networking-statistics/; last access: August, 2014.

Toch, E., Cranshaw, J., Hankes-Drielsma, P., Springfield, J.; Gage, P., Cranor, L.; Hong, J., Sadeh, N., 2010. Locaccino: A Privacy-centric Location-sharing Application. In *12th ACM International Conference Adjunct Papers on Ubiquitous Computing*, pp. 381-382.

Benisch, M.; Kelley, P. G., Sadeh, N., Cranor, L. F., 2011. Capturing Location-Privacy Preferences: Quantifying Accuracy and User-Burden Tradeoffs, In *Personal and Ubiquitous Computing*; vol. 15, pp. 679-694, 2011.

Toch, E., Cranshaw, J., Drielsma, P. H., Tsai, J. Y., Kelley, P. G., Springfield, J., Cranor, L., Hong, J.; Sadeh, N., 2010. Empirical Models of Privacy in Location-sharing. In *12th ACM International Conference on Ubiquitous Computing*, pp. 129-138.

Smith, I., Consolvo, S., Lamarca, A., Hightower, J., Scott, J., Sohn, T., Hughes, J., Iachello, G., Abowd, G. D., 2005. Social Disclosure of Place: From Location Technology to Communication Practices. In *Third International Conference on Pervasive Computing*, pp. 134-151.

Ribeiro, F. N., Zorzo, S. D., 2009. LPBS – Location Privacy Based System. In *IEEE Symposium on Computers and Communications*, pp. 374-379.

Shin, K. G., Ju, X., Chen, Z., Hu, X., 2012. Privacy Protection for Users of Location-Based Services. In *IEEE Wireless Communications*, vol. 19, pp. 30-39.

Harrison B., Dey, A., 2009. What Have You Done With Location-Based Services Lately?. In *IEEE Pervasive Computing*, vol. 8, pp. 66-70.

Bilogrevic, I., Huguenin, K., Agir, B., Jadliwala, M., Hubaux, J. P, 2013. Adaptive Information-sharing for Privacy-aware Mobile Social Networks. In *2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pp. 657-666.

Xu, F., He, J., Wright, M., Xu, J., 2010. Privacy Protection in Location-Sharing Services. In *International Conference on Computer Application and System*

Modeling, ICCASM.

Android; http://www.android.com; Last access: November, 2013.

Dierks, T., Rescorla, E., 2013. The Transport Layer Security (TLS) Protocol. RFC (Request for Comments) 4346. Available: http://www.ietf.org/rfc/rfc4346.txt. Last access: November, 2013.

Leon, P. et al. Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising. In: *SIGCHI Conference on Human Factors in Computing Systems*. New York, NY, USA. Pages 589-598. 2012

Hochbaum, D. S., Shmoys, D. B., 1985. A Best Possible Heuristic for the K-center Problem. *Math. of Oper. res*., Vol. 10, No. 2, pp. 180-184.

Smart, S. W., 1977. TextBook on Spherical Astronomy., 6. ed*., England: Cambridge University Press*, 415 p.

Williams. Ed. Aviation Formulary 1.44. Available: http://williams.best.vwh.net/avform.htm#LL; Last access: November, 2013.

Gao, H. et al. Security issues in online social networks. In: *IEEE Internet Computing*, 15(4), pp. 56–63. 2011

SCITEPRESS
SCIENCE AND TECHNOLOGY PUBLICATIONS